Post-Quantum Cryptography: Overview and IoT Standardisation Perspectives

T2TRG Interim Meeting
Tuesday 21th May 2024 @ Paris

Renzo E. NAVAS
Outline

1. Background
2. Key Encapsulation Methods (KEMs)
3. Digital Signatures (DS)
4. T2TRG/IETF SoA and Next Steps?
The Quantum Threat

• ... Non-zero probability of existence of a large-scale quantum computer in the next 50y, better be prepared (Pascal's wager)

• **Shor’s algorithm:**
  A large quantum computer could solve the *discrete logarithm* and *factorization* problems in *polynomial time* (very efficiently)
  o This breaks: RSA, (EC)DSA, (EC)DH
  o Essentially, all *currently-used asymmetric cryptography*

• **Grover’s algorithm:**
  An extremely large quantum computer could solve the *exhaustive search* problem in *square-root* time (somewhat efficiently)
  o This is a generic attack against any possible cryptographic algorithm (in particular, *all symmetric-key cryptography is affected*)
  o However, the attack remains inefficient
Quantum-Safe Cryptography

• Symmetric crypto: use longer keys

• Asymmetric crypto
  o Solution: abandon discrete logarithm & factorization and use **algorithms relying on other mathematical problems**
  o Three main families: **Lattice-**, **Codes-**, and **Hash-based**

• Post-Quantum Cryptography (PQC)
  • Stands for protocols, algorithms, and mathematical problems that are hard to solve even for a quantum computer
  • ... runs on current Hardware
  • "Quantum cryptography" (quantum physics-based) exists in the form of Quantum Key Distribution (not mature yet), I will not talk about this.
NIST PQC Standardization Process

• Started in 2016, ongoing – www.nist.gov/pqcrypto
  o Digital Signatures (DS):
    ▪ 3 + Ongoing (New Round 1): 40 candidates
  o Public-key Encryption and Key-Establishment Algorithms (KEM):
    ▪ 1 + Ongoing (Final Round 4): BIKE, Classic McEliece, HQC, and SIKE

<table>
<thead>
<tr>
<th>PQC-Family</th>
<th>Type</th>
<th>Name</th>
<th>Drafts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice</td>
<td>KEM</td>
<td>ML-KEM</td>
<td>Draft FIPS 203 (CRYSTALS-Kyber)</td>
</tr>
<tr>
<td></td>
<td>DS</td>
<td>ML-DSA</td>
<td>Draft FIPS 204 (CRYSTALS-Dilithium)</td>
</tr>
<tr>
<td></td>
<td>DS</td>
<td>FN-DSA</td>
<td>FALCON</td>
</tr>
<tr>
<td>Hash-based</td>
<td>DS</td>
<td>SLH-DSA</td>
<td>Draft FIPS 205 (SPHINCS*)</td>
</tr>
</tbody>
</table>

Table: NIST’s PQC standards as of May 2024
Key Encapsulation Methods (KEMs)
KEMs

- FIPS 203: Module-Lattice-based Key-Encapsulation Mechanism (ML-KEM)
  - AKA “Kyber”
- Also NIST, three non-lattice-based: BIKE, Classic McEliece, HQC

- A Key Encapsulation Method (KEM) is a three-tuple of algorithms [1]:
  - Key Generation() --> ek, dk
  - Encapsulate(ek) --> K, c
  - Decapsulate(dk, c) --> K

A Simple KEM (no authentication!)

ALICE

KEY GENERATION

Private Key

Public Key

Shared Secret

DECAPSULATION

Private Key

Public Key

Bob

Shared Secret

ENCAPSULATION

ciphertext

PQC: Overview and IoT Std. Perspectives (Renzo NAVAS).
T2TRG. 21th May 2024 @ Paris
KEMs : Communication Cost

- **PK (Bytes)**: Public key or transmitted output of the key generation algorithm
- **CT (Bytes)**: Ciphertext or transmitted output of the key encapsulation algorithm
- **Cat 1 / 3 / 5**: NIST security categories, equivalent to the strength of a block cipher with a 128/192/256-bit key

<table>
<thead>
<tr>
<th>Scheme</th>
<th>PQC-family</th>
<th>PK Cat 1</th>
<th>CT Cat 1</th>
<th>PK Cat 3</th>
<th>CT Cat 3</th>
<th>PK Cat 5</th>
<th>CT Cat 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML-KEM (Kyber)</td>
<td>Lattice</td>
<td>800</td>
<td>768</td>
<td>1184</td>
<td>1088</td>
<td>1568</td>
<td>1568</td>
</tr>
<tr>
<td>BIKE (Bit Flipping Key Encapsulation)</td>
<td>Code</td>
<td>1541</td>
<td>1573</td>
<td>3083</td>
<td>3115</td>
<td>5122</td>
<td>5154</td>
</tr>
<tr>
<td>McEliece</td>
<td>Code</td>
<td>261120</td>
<td>128</td>
<td>524160</td>
<td>188</td>
<td>1044992</td>
<td>240</td>
</tr>
<tr>
<td>HQC (Hamming Quasi-Cyclic)</td>
<td>Hash</td>
<td>2249</td>
<td>4497</td>
<td>4522</td>
<td>9042</td>
<td>7245</td>
<td>14485</td>
</tr>
</tbody>
</table>

Digital Signatures (DS)
DSs: Communication Cost

Three Algorithms: KeyGen(), Sign(sk, M), Verify(pk, M, σ)

Legend:
- PK (Bytes): Public key or transmitted output of the key generation algorithm
- Sig (Bytes): Signature or transmitted output of the Sign algorithm
- Cat 2: NIST security category, equivalent to the collision-search strength of a 256-bit hash function (e.g., SHA-256)
- Cat 1/3/5: NIST security categories, equivalent to the key-search strength of a block cipher with a 128/192/256-bit key

<table>
<thead>
<tr>
<th>Scheme</th>
<th>PQC-family</th>
<th>PK Cat 1</th>
<th>Sig Cat 1</th>
<th>PK Cat 2</th>
<th>Sig Cat 2</th>
<th>PK Cat 3</th>
<th>Sig Cat 3</th>
<th>PK Cat 5</th>
<th>Sig Cat 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML-DSA (Dilithium)</td>
<td>Lattice</td>
<td>-</td>
<td>-</td>
<td>1312</td>
<td>2420</td>
<td>1952</td>
<td>3293</td>
<td>2592</td>
<td>4595</td>
</tr>
<tr>
<td>FN-DSA (FALCON)</td>
<td>Lattice</td>
<td>897</td>
<td>666</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1793</td>
<td>1280</td>
</tr>
<tr>
<td>SLH-DSA - small (SPHINCS+)</td>
<td>Hash</td>
<td>32</td>
<td>7856</td>
<td>-</td>
<td>-</td>
<td>48</td>
<td>16224</td>
<td>64</td>
<td>29792</td>
</tr>
</tbody>
</table>

T2TRG/IETF SoA and Next Steps?
IETF PQC State of the Art / Efforts

• Post-Quantum Use In Protocols (PQUIP) WG
  • “The WG will provide a standing venue to **discuss PQC** (operational and engineering) transition issues and experiences to date relevant to work in the IETF”
  • [https://datatracker.ietf.org/wg/pquip/about/](https://datatracker.ietf.org/wg/pquip/about/)

• Hybridation (Transitioning Phase)
  • Hybrid KEMs
    • Hybrid Public Key Encryption (HPKE) [https://datatracker.ietf.org/doc/rfc9180/](https://datatracker.ietf.org/doc/rfc9180/)
  • Hybrids DS:

---

PQC: Overview and IoT Std. Perspectives (Renzo NAVAS).
T2TRG. 21th May 2024 @ Paris
KEMs IoT-Friendly? (1)

- Step 1: Standardize PQC KEMs COSE’s Encoding (COSE WG)
  - In particular, ML-KEM (Kyber):
    - Talked with Orie in IETF 118 Prague, he was OK that I took on/revive
    - Seems that team is focusing on SLH-DSA (SPHINCS+)

- I just discovered that IETF work is being done since 5th March 2024 :’)
  and was discussed at IETF 119 (draft targeting JOSE/COSE)
  - COSE ML Discussion: [https://mailarchive.ietf.org/arch/browse/cose/?q=draft-reddy-cose-jose-pqc-kem-00&gbt=1](https://mailarchive.ietf.org/arch/browse/cose/?q=draft-reddy-cose-jose-pqc-kem-00&gbt=1)
  - Presentation IETF 119 JOSE: [https://youtu.be/drpDw4moGuE?si=HcIsIYysXhqFHg2r&t=2892](https://youtu.be/drpDw4moGuE?si=HcIsIYysXhqFHg2r&t=2892)
  - I will contact Tirumal/Aritra/Hannes ... see if I can help (?) ...
KEMs IoT-Friendly? (2)

• Step 2: Instantiate ML-KEM over IoT-friendly solution (...CoAP)
  • In the same line as EDHOC (RFC 9528)
  • **Fragmentation!** Handled by CoAP? (Block transfer) – Crypto guarantees?
  • **Authentication**: ML-KEM is not authenticated, MoM trivial – Std. on AM?
  • OSCORE/LAKE WG?

• Step 3 (?): Hybridation/Hybrid Public Key Encryption (RFC9180)
  • Hannes, Orie, Ajitomi and Laurence are on that: https://datatracker.ietf.org/doc/draft-ietf-cose-hpke/07/
  • See also https://datatracker.ietf.org/doc/draft-ajitomi-cose-cose-key-jwk-hpke-kem/ (expired)
T2TRG Vision/Next Steps?

• ... Quantum Resilient IoT
  • Use Cases, Minimum Node/Network requirements?

• Are our PQC efforts fragmented?
  • Seems so, because hot-topic
  • PQUIP WG is enough? ... apparently not
    • “The output of this WG is expended to inform protocol work and guidance developed by other WGs in the IETF.”
    • How we align, at least within IoT community? (... Hannes is nearby?)

• Wait and adapt from “big-brothers” to constrained IoT/T2T?
  • E.g., ACE framework requirements to be Quantum-Resilient? (Certificates/Tokens, Key-related topics, Quantum-Resilient Profile for ACE)

• .... Personally, I would like to have an Authenticated ML-KEM suitable for IoT nodes (Cortex-M0/M3? LPWAN?) soon
Thank you!
Discussion?

renzo.navas@imt-atlantique.fr
References

1. ANSSI views on post-quantum transition - Jérôme Plût. 2023-11-07 PKIC Post-Quantum Cryptography Conference
2. NIST FIPS 203 (Draft) Federal Information Processing Standards Publication Module-Lattice-based Key-Encapsulation Mechanism Standard
Appendix
## NIST Security Strength Categories

<table>
<thead>
<tr>
<th>Security Category</th>
<th>Corresponding Attack Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Key search on block cipher with 128-bit key</td>
<td>AES-128</td>
</tr>
<tr>
<td>2</td>
<td>Collision search on 256-bit hash function</td>
<td>SHA3-256</td>
</tr>
<tr>
<td>3</td>
<td>Key search on block cipher with 192-bit key</td>
<td>AES-192</td>
</tr>
<tr>
<td>4</td>
<td>Collision search on 384-bit hash function</td>
<td>SHA3-384</td>
</tr>
<tr>
<td>5</td>
<td>Key search on block cipher with 256-bit key</td>
<td>AES-256</td>
</tr>
</tbody>
</table>
Pointers on Kyber Research and Implem.

**Implementation for embedded devices** - References

- PQM4: Collection of post-quantum cryptographic algorithms for the ARM Cortex-M4:
  - [https://github.com/mupq/pqm4](https://github.com/mupq/pqm4)
- Compact Dilithium Implementations on Cortex-M3 and Cortex-M4
  - [https://github.com/dilithium-cortexm/dilithium-cortexm](https://github.com/dilithium-cortexm/dilithium-cortexm)
  - [https://doi.org/10.46586/tches.v2021.i1.1-24](https://doi.org/10.46586/tches.v2021.i1.1-24)
  - 4y old, but Cortex-M3

**Research Articles (RQ1 : PQ KEM on IoT possible?)**

- Partial results for Systematic Review November 2023
- 77 articles mentioning implementation of Kyber
- Of the 22 summarized, only ONE implemented it on a real (non-constrained) network

(Partial Takeaway) The research community focus on computation optimization / benchmarking, not much on the distributed communication cost (energy, real messages)

Fig: Partial View of our Systematic Literature Review Process

PQC: Overview and IoT Std. Perspectives (Renzo NAVAS).
T2TRG. 21th May 2024 @ Paris
Baby Kyber: Learning Kyber’s Math

- Baby Kyber: A simple implementation of Kyber (n: 256 → 4)
- Main Author: Juan Ignacio Migliorisi (UBA)
- Jupyter Notebook (... Google collab):
  - https://colab.research.google.com/drive/1c1OPJHGKoVcTYd8ymYq6NCCp9ISuf_Ve#scrollTo=Zf6bMpQW-36i

In our baby kyber example we consider:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>4</td>
</tr>
<tr>
<td>q</td>
<td>17</td>
</tr>
<tr>
<td>k</td>
<td>2</td>
</tr>
</tbody>
</table>

note that q is a prime number and chosen to be equal to $2^n + 1$
Kyber Background

The Learning With Errors (LWE) problem

- Errors are noise vectors sampled from a Centered Binomial Distribution

- \( k \times k \) multiplications, where each element is a grade \( n \) polynomial mod \((x^n + 1)\) → a lot of time!

- each coefficient is an integer mod \( q \) (\( q \) is a prime)

- Number Theoretic Transform (NTT) solves this in \( O(n \log n) \) time

\[
\sum_{i=0}^{n-1} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}
\]
Kyber Side Notes

• Kyber computational Cost: Notably, that he uses the NTT (Number Theoretic Transform) and thus no need for processors with floating point unit (<= Cortex M3, so that is good), can be accelerated in HW in the future

• What is the current understanding of the security of Kyber512 (i.e., ML-KEM-512)

• Research community mostly focus on in-node performance and not on the networking aspects of the protocols.
Hybridation

• The hybridation consists in combining two (or more) cryptographic schemes achieving the same functionality in a robust way.

• In other words, the combination should be secure in the classical/quantum computation model as long as one underlying scheme is secure in that model.

• KEM Hybridation
  • Draft for PQC TLS option with an hybridation mode using concatenation and KDF - https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
  • IKEv2 is also evolving to include hybrid post-quantum cryptography. RFC 9370 - https://datatracker.ietf.org/doc/html/rfc9370

• DS Hybridation: less mature